## REMARKS

This responds to the Office Action mailed on April 14, 2005, and the references cited therewith.

Claims 26, 32, 38, 44, and 47 are amended, claim 1-25 are canceled and as a result, claims 26-47 are now pending in this application.

*§102 Rejection of the Claims*

Claims 26-47 were rejected under 35 U.S.C. § 102(e) as being anticipated by Spies et al. (U.S. Patent No. 6,055,314).

The Examiner asserts that Spies et al. discloses the invention claimed in claims 26, 38 and 47. The Applicant disagrees for the reasons set forth.

The Spies reference describes a method wherein a content purchaser presents a card to a merchant for authentication. If the card is authenticated, a cryptographic key for a selected video is transferred to the card. The Spies reference describes a use of IC cards which require a direct insert into a reader to be read. This is in contrast to what is claimed.

What is claimed herein is: A method of acquiring and playing digital content comprising: acquiring a physical unmodifiable key containing a unique key code from a key provider; requesting digital content from a content provider wherein the key code from the key provider is usable for more than one download of more than one type of digital content from more than one content provider;

after locking the digital content with an unlock code associated with the key code contained in the physical key, receiving the locked digital content; and

entering the locked digital content into a playing device having a reader-decoder circuit capable of decryption that reads the key code and determines whether the key code is associated with the unlock code, the device being enabled to unlock code, and play the digital content if the key code is associated with the unlock code, the key being a physical object adapted to be carried and wirelessly used by a user apart from the playing device.

The claimed invention includes a key, that can be carried and wirelessly used by a user apart from a playing device, that permits users to protect multiple pieces and types of content concurrently, while also securing hard drives, online banking/credit card transactions and access to physical items. This functionality cannot be achieved by the Spies reference which requires a use of IC cards that are capable of protecting only one piece of content at a time. The IC cards are not wireless and require a card reader for use. Furthermore, the IC card described in the Spies reference does not protect multiple pieces and types of content concurrently. Instead, the IC card protects only one piece of content at a time.

The IC card security described in the Spies reference depends upon key stores to provide a new key for each new use. The claimed invention does not have this key store requirement at all. As claimed, a physical unmodifiable key containing a unique key code from a key provider is all that is required because the unique key code from the key provider is usable for more than one download of more than one type of digital content from more than one content provider.

Unlike the method described in the Spies reference, the method embodiments claimed herein are able to simultaneously protect unlimited pieces of content, because the key code from the key provider is usable with more than one type of digital content from more than one content provider and wherein the key code accessibility is wireless. In the Spies reference, a different cryptographic key is associated with each type of content. In the claimed invention, it is not required that any cryptographic key be downloaded with the unmodifiable key. The claimed invention does not require a crypto key to be downloaded at all.

The Spies reference describes IC cards that are modified as a part of each transaction. The key claimed herein is not modified. As a result, the claimed key is assignable to a user and permanently identified whenever used by that individual. The model IC cards in the Spies reference cannot be utilized in this manner. Instead, the Spies system requires another element (which must be run and maintained by merchants), a key store, for operation.

Furthermore, the Spies device specifies that the content decryption functionality is preferably contained in the IC card (*helped* by the STB's processor only when needed). Because of the quantity of data and level of processing required in a typical decryption cycle, this design choice prohibits Spies' IC cards from functioning wirelessly. In fact, it requires the keys to be physically inserted into a physical card reader in order to function. This design choice also requires the IC cards to incorporate relatively high-powered data transmission channels/paths and processing capabilities, neither of which is required in the claimed invention, as decryption (in the claimed invention) always occurs in the playing device, not the keys.

The Spies reference describes a video content player to be delivered with an I/O card reader. The claimed invention does not use an I/O card reader as the key is a "physical object adapted to be carried and wirelessly used by a user apart from the playing device."

The Examiner, in discussing claim 37, attempts to equate the "wireless" transmission from an earth orbiting satellite to a television's set-top-box receiver (as referred in Spies), to the wireless transmission of a key code from a wireless key to a playing device (as referred in the claimed invention). The Applicant asserts that the satellite transmissions referenced in Spies are completely unrelated to the wireless key transmissions of the claimed invention.

Additionally, content decryption in the Spies reference takes place in the IC card itself. In the claimed invention, content decryption takes place in the receiver-decoder circuit (RDC.)

Because the Spies et al. reference does not include each and every element claimed, the Spies et al. reference does not anticipate claims 26- 47.

## CONCLUSION

Applicant respectfully submits that the claims are in condition for allowance, and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney at (612) 373-6976 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

Respectfully submitted,

JOHN J. GIOBBI

By his Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402
(612) 373-6976

Date 11 May 05

By _____
Janal M. Kalis
Reg. No. 37,650

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop Amendment, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 11th day of May, 2005.

CANDIS BUENDING

Name

Signature